



# HIPAA Security and Documentation

## 45 CFR §164.316

H I P A A   S e c u r i t y ♦ S e p t e m b e r   2 0 0 5

### ***Purpose***

While documentation rules are not new to health care, the Security Rule adds additional requirements for TRICARE Management Activity (TMA), Military Treatment Facilities (MTFs) and Dental Treatment Facilities (DTFs) to ensure the confidentiality, integrity and availability of individual's electronic Protected Health Information (ePHI). TMA, MTFs, DTFs and other Department of Defense (DoD) covered entities must document their implementation of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule in order to ensure accountability for the covered entity's security practices. Policies, procedures and other documentation are needed to support a decision made by the covered entity in an investigation of an individual's complaint, security breach or to demonstrate compliance with the Rule.

### ***Policy***

Policies and procedures related to ensuring the confidentiality, integrity and availability of individually identifiable health information in electronic format must be maintained in either written or electronic form. Covered entities must document and maintain in either written or electronic form a record of any actions, activities, or designations required by the Security Rule. All required documentation must be maintained for a period of six years and made available to those who are responsible for implementing the procedures to which the documentation pertains, or need access to the information in the course of carrying out their legally authorized duties. MTFs, DTFs and other DoD covered entities are to periodically review and update all required documentation to ensure its accuracy and appropriateness.

### ***Documentation Related to Policies and Procedures***

MTFs, DTFs and other DoD covered entities must document the policies and procedures used to implement the Security Rule. This ensures consistency and accountability for the implementation of safeguards used to protect electronic protected health information (ePHI) and comply with the standards and implementation specifications of the Security Rule. The Security Rule requires the use of risk analysis and a risk management process in the selection of those safeguards to ensure that they are reasonable and appropriate. This process must balance the size, complexity, and capabilities of the covered entity, the technical infrastructure, hardware and software capabilities, and the costs of security measures against the perceived probability and criticality of the risks as determined through the risk assessment process, including the costs and potential damage to the covered entity and individuals whose personal information may be disclosed, altered or destroyed as a result of a security breach or policy violation. The selection process including justification for decisions to implement addressable implementation specifications or alternatives must be documented.

PrivacyMail@tma.osd.mil • [www.tricare.osd.mil/tmaprivacy](http://www.tricare.osd.mil/tmaprivacy)



# HIPAA Security and Documentation

## 45 CFR §164.316

H I P A A   S e c u r i t y ♦ S e p t e m b e r   2 0 0 5

### ***Documentation Related to Actions, Activities, and Designations***

MTFs and other DoD covered entities must document any actions, activities and designations required by the Security Rule. This ensures accountability by those responsible for the security of ePHI and demonstrates due diligence and compliance by those responsible for implementing policies and procedures. Required actions, activities and designations include but are not limited to:

Assigned Security Responsibility. Designate in writing the security official responsible for the development and implementation of the policies and procedures required by the Security Rule. Appointment letters should include assigned areas of responsibility and duties.

Risk Analysis. Document the results of the process used to assess the potential risks and vulnerabilities to the confidentiality, integrity and availability of ePHI created, used and stored by the covered entity.

Access Establishment and Modification. Document each user's access rights to workstations, transactions, programs or processes based on access authorization policies that are consistent with the minimum necessary policies established through implementation of the DoD Health Information Privacy Regulation, DoD 6025.18-R.

Security Incident Response and Reporting. Document suspected and known security incidents and their outcomes. Reports should include the details of the incident, how the incident was responded to, investigation results, corrective actions and actions taken to mitigate harmful effects.

Evaluation. Document the results of periodic technical and non-technical evaluations that establish the extent policies and procedures comply with the Security Rule requirements. Following the initial evaluation establishing compliance, subsequent evaluations should be conducted whenever environmental or operational changes affecting the security of ePHI have occurred.

Business Associate Contracts and Other Arrangements. Document the satisfactory assurances that business associates will appropriately safeguard ePHI through written contracts or other written arrangements such as Memoranda of Understanding or Agreement that meet the applicable requirements of the Security Rule.

Maintenance Records. Document the repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls,



# HIPAA Security and Documentation

## 45 CFR §164.316

### H I P A A   S e c u r i t y ♦ S e p t e m b e r   2 0 0 5

doors and locks). Records should include who made the repairs or modifications, what work was done and when.

Workstation Use. Document the authorized use for workstations that access ePHI. For each workstation or class of workstation specify the proper functions that may be performed, the manner in which they may be performed and the physical attributes of the surroundings. For example, workstations located in a patient's hospital room must not face a window or open doorway and may only be used by authorized personnel to enter data (patient status, treatment, etc.) relating to the individual occupying that room during regular duty hours.

Device and Media Controls. Document the movement of any hardware and electronic media and the person responsible. Records should include the current location of hardware and electronic media and the person responsible for it, date and time they are moved and the person responsible for that movement, and the new location and person responsible for it.

Data Backup and Storage. Document the creation of backups before equipment is moved.

Unique User Identification. Document the assignment of a unique name and/or number to each user to identify and track user identity and actions.

Audit Controls. Record and examine activity in information systems that contain or use ePHI. Document the results of the information systems activity reviews and maintain that documentation and the original logs or records related to any security incidents, anomalies or suspicious activity noted in the review.